RMT:JAM/JGH

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AND DESCRIBED AS 4956 STATE ROUTE 52, JEFFERSONVILLE, NEW YORK 12748 AND ALL CLOSED AND LOCKED CONTAINERS	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20 MJ 426

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Colin J. McLafferty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the premises known and described as 4956 State Route 52, Jeffersonville, New York 12748, and any closed and locked containers found therein, described in Attachment A (the "Target Premises"), for the evidence, fruits and instrumentalities of federal criminal law described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since July 2018. Since 2019, I have been assigned to the FBI's Joint Terrorism Task Force ("JTTF"). I have investigated crimes involving, among other things, terrorism and the illegal possession of firearms.

3. The JTTF is investigating DZENAN CAMOVIC and others for an attack on multiple New York City Police Department ("NYPD") officers on or about June 3, 2020. The investigation involves violations of, among other statutes, 18 U.S.C. § 231(a)(3) (obstruction of

law enforcement officer related to civil disorder),[1] 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien), 18 U.S.C. § 1951 (Hobbs Act robbery), 18 U.S.C. § 924(c) (discharge of a firearm during a crime of violence) and 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization) (collectively, the "Subject Offenses")

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where the contents of documents and written communications are summarized herein, they are done so in sum and substance and in pertinent part unless otherwise indicated.

JURISDICTION

5. The Target Premises are located in the Southern District of New York. The Court has the authority to issue the attached warrant pursuant to Federal Rule of Criminal Procedure 41(b)(3), which states that a federal magistrate judge has authority to issue a search warrant "in an investigation of domestic terrorism or international terrorism – with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district."

BACKGROUND ON ISIS

6. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq ("AQI"), then known as Jam'at al Tawhid wa' al-Jihad, as a Foreign Terrorist

---

[1] Section 231(a)(3) provides, in relevant part: "(3)Whoever commits or attempts to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays, or adversely affects commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function—Shall be fined under this title or imprisoned not more than five years, or both."

Organization ("FTO") under Section 219 of the Immigration and Nationality Act, and as a Specially Designated Global Terrorist entity under Section 1(b) of Executive Order 13224. On or about December 11, 2012, the Secretary of State amended the designation of AQI to include the following aliases: al-Nusrah Front ("ANF"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

7. On or about May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between ANF and AQI, amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224, to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name and to remove all aliases associated with al-Nusrah Front. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham (ISIS - which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the ISIS FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

8. Based on my training and experience, my personal participation in this and other investigations involving ISIS, my conversations with other law enforcement agents who have been involved in ISIS-related investigations, and my review of publically available materials, I have learned that to gain supporters, ISIS, like many other terrorist organizations, spreads its message

using social media, Internet platforms, and sites on the "dark web."[2] Using these platforms, ISIS posts and circulates videos and updates of events in Syria, Iraq, and areas with an ISIS presence, in English and Arabic, as well as other languages, to draw support to its cause.

9. Most recently, based on publically available materials, I have learned that ISIS supporters have taken an interest in the rioting, looting and other violence attendant to the series of largely-peaceful demonstrations and protests throughout the United States in or about late May 2020 and early June 2020, and has directed ISIS supporters to commit acts of violence in the United States during this period of time. Specifically, pro-ISIS social media accounts have featured police cars burning and other violent imagery. For example, on "Shamukh," which is an ISIS-related forum on the dark web, a series of threads on or about May 31, 2020 urged supporters in the United States to exploit current social tensions by carrying out physical attacks against law enforcement and protesters to sow further discord.

PROBABLE CAUSE

THE JUNE 3, 2020 ATTACK

10. On or about June 3, 2020, at approximately 11:50 p.m., CAMOVIC approached two uniformed NYPD officers in the vicinity of 885 Flatbush Avenue in Brooklyn, New York. Security camera footage from the area shows CAMOVIC walking on Flatbush Avenue toward the intersection of Flatbush and Church Avenues. Upon reaching the corner of Flatbush and Church Avenues, CAMOVIC turned onto Church Avenue, where the two NYPD officers stood

[2] The dark web is content that exists on the Internet but is not indexed by traditional search engines. Dark web content requires specific software or applications to access, such as TOR, or "The Onion Router," which was used by CAMOVIC and described below.

on patrol. The surveillance video shows that, upon turning the corner in the direction of the police officers, CAMOVIC immediately stabbed one of officers in the neck area with a knife he already had in his hand, and then began chasing the second officer, repeatedly and violently stabbing at the officer and eventually throwing his knife at the officer. CAMOVIC then ran back toward the first officer, whom he had already stabbed, and again attacked the officer.

11. A struggle ensued. Video footage from the officer's body camera shows that CAMOVIC fought for control of the officer's service weapon. CAMOVIC ultimately gained control of the weapon and fired multiple shots at several officers, including at one or more officers who responded to the scene.

12. CAMOVIC was ultimately shot by responding officers and taken into custody. The officer's service weapon used by CAMOVIC, a SIG Sauer P226 black semiautomatic 9mm handgun, was recovered from the scene. Law enforcement officers searched CAMOVIC's person incident to his arrest, during which time they recovered a black LG smart cellular phone (the "CAMOVIC LG Phone").

13. Based on my training and experience, I know that the NYPD has a presence, and employs police officers and other employees that operate in their official capacity, in multiple locations outside of New York state and outside of the United States.

14. I have also conferred with an Interstate Nexus expert with the Bureau of Alcohol, Tobacco, Firearms, and Explosives, who has informed me, in substance and in part, that the officer's service weapon was manufactured outside the state of New York.

CAMOVIC'S POSSESSION OF ISIS AND JIHADIST PROPOGANDA AND USE OF OPERATIONAL SECURITY

15. On the video footage from a police officer's body camera, CAMOVIC can be heard repeatedly yelling "Allahu Akbar" during the attack. Based on my knowledge, training and experience, I know that "Allahu Akbar" is an Arabic phrase that means "God is the greatest" and has been shouted by perpetrators of violent jihadist attacks during such attacks.

16. Following his June 3, 2020 attack on police officers, law enforcement agents recovered several cell phones, electronic devices and electronic storage media ("the Devices") from CAMOVIC's bedroom at his father's apartment in Brooklyn, New York. Notably, while the sleeve for a laptop computer was also found in CAMOVIC's bedroom, but no laptop was located inside of the apartment.

17. Pursuant to court-authorized search warrants, a review of the content of the Devices found in CAMOVIC's room indicates that CAMOVIC is a consumer of extremist and violent jihadist media. In particular, the content includes propaganda materials issued by or associated with ISIS.

18. Among the Devices recovered from CAMOVIC's room were several compact discs ("CDs") or digital video discs ("DVDs"). The labels of these discs indicated that they contained violent jihadist content. For example, several were marked "Anwar al-Awlaki," including one that also included the word "jihad." Al-Awlaki was a United States-born radical Islamic cleric and prominent leader of al-Qaeda in the Arabian Peninsula ("AQAP") who was killed on or about September 30, 2011. Even now, nearly nine years after his death, al-Awlaki is still commonly regarded as the leading figure inciting English-speaking Muslims to participate in violent jihad.

19. Another of the Devices found in CAMOVIC's bedroom, a 64-gigabyte thumb drive, was found sitting on top of a copy of the Quran. An examination of the device by law enforcement revealed that the device contained numerous files, as well as files that were deleted or otherwise attempted to have been removed from the thumb drive, that are related to jihadist propaganda, as well as ISIS-related propaganda. For example, one file found on the thumb drive is titled "The Dust Will Never Settle Down," and contains an audio recording of a speech of the same name by al-Awlaki. In the speech, al-Awlaki advocated violence against individuals that he believed defamed and mocked Islam. Another file, titled "Constants on the Path of Jihad" is another speech by al-Awlaki where he argued that the concept of "jihad" denoted violent combat against disbelievers rather than an internal struggle. Particularly relevant to CAMOVIC's attack is another file on the thumb drive titled "Stop Police Terror," which is another speech by al-Awlaki. Several files found in the examination of the thumb drive bore logos of official ISIS media outlets.

20. The thumb drive from CAMOVIC's bedroom contained other materials specifically related to, or created by ISIS. For example, the thumb drive contained a file "Saleel al Sawarim," which I understand translates roughly into English as "The Clanging of Swords."

21. A forensic examination of the above-described thumb drive also recovered artifacts and data related to ISIS and violent jihadist propaganda, which indicates that these files were once on the drive but are no longer accessible, which often indicates that an individual attempted to delete or remove these files.

22. For example, the thumb drive contained files with logos of al-Hayat Media Center, al-Ajnad, al-Bayan, which are all official ISIS media outlets. Further, the thumb drive contained images bearing Arabic-language logos which said "The Islamic State," and "Dabiq,"

the name of a town in Syria and ISIS's now-defunct magazine. A file titled "Shaheed for the sake of Allah," but whose content is no longer accessible, was also found. Based on my training and experience, I know that "shaheed" is an Arabic word that means "martyr" and is often used by supporters of ISIS and other foreign terrorist organizations to refer to individuals who die while committing an act of terrorism in support of the organization. Based on my training and experience I also know that "For the sake of Allah" is a phrase taken from the Quran and often used by violent Salafi Muslims to describe their path in life.

23. As another example, another file title that is no longer accessible on the thumb drive contains Arabic writing I understand translates to "The Sheikh Adnani." Based on my training and experience, I believe that "Sheikh Adnani" likely refers to Sheikh Abu Muhammad al-Adnani, who is the now-deceased former spokesman and senior official of ISIS. Notably, in a September 22, 2014 speech entitled "Indeed Your Lord is Ever Watchful," Adnani stated that Muslims wishing to attack non-believers should not ask permission nor seek anyone's approval. Adnani stated disbelievers' blood was "halal," or permitted, for the Muslims. Regarding attack methods against a disbeliever, Adnani emphasized a lack of resources for a sophisticated attack was not a barrier. Regarding the disbeliever, Adnani stated "Smash his head with a rock, or slaughter him with a knife, or run him over with your car."

24. Much of the aforementioned extremist and jihadist content found on the thumb drive, CDs and DVDs was also found on a Samsung cell phone in CAMOVIC's room. This phone had two of CAMOVIC's email accounts synced to the phone, indicating that it was, in fact, used by CAMOVIC.

25. Based on my training and experience, I know that individuals involved in terrorist activity, or who support foreign terrorist organizations like ISIS, will often try to delete or erase data related to their activity in order to evade detection by law enforcement.

26. Pursuant to a court-authorized search warrant, law enforcement officers conducted a search of the CAMOVIC LG Phone. A preliminary review of the CAMOVIC LG Phone has revealed that CAMOVIC downloaded and used an application called Orbot. Orbot is a mobile application used for the Tor network. Tor, in turn, is a computer network designed to facilitate anonymous communication over the Internet. The Tor network accomplishes this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering ineffective any conventional Internet Protocol ("IP") address-based methods of identifying users. To access the Tor network, a user installs specific Tor software. The Tor network also enables users to operate hidden sites that operate similarly to conventional websites. The Tor network permits a user to conduct internet activity with a high degree of privacy and anonymity. As a result, the network is often used by individuals involved in criminal activity that want to obscure their identity and evade law enforcement.

27. Here, it appears that CAMOVIC downloaded and began using Orbot to connect to the Tor network on or about June 1, 2020—two days prior to his attack. CAMOVIC appears to have connected and used the application on several occasions thereafter. On or about June 2, 2020 at approximately 10:00 p.m. New York time—less than 24 hours before the attack—CAMOVIC deleted the application. It appears that CAMOVIC may have been attempting to delete evidence of his criminal activity.

28. Additionally, the review of the CAMOVIC LG Phone also indicates that CAMOVIC downloaded and used a mobile application called Citizen shortly before the

attack. Citizen is a social media application that allows users to send and receive information about local events associated with law enforcement activity. According to its website, Citizen describes itself as a "safety app that give you instant access to verified 911 information."

29. A user of the Citizen application located in or around the New York City region would receive alerts and information pertaining to NYPD law enforcement activity. In particular, during the relevant time period, a user of the Citizen application would have received information about NYPD activity related to the ongoing protests, looting and civil disorder. The application also allows users to submit and upload information and videos pertaining to such activity. The application provides mapping and location information for these events, and so a user would be able to learn about locations where NYPD are present.

30. CAMOVIC downloaded the Citizen application on June 2, 2020 and accessed the application on several occasions prior to his attack, including on June 3, 2020, shortly before the attack on law enforcement.

31. Additionally, according to records provided by the company that operates Citizen, CAMOVIC's service with Citizen began on or about May 26, 2018, which indicates that CAMOVIC utilized Citizen on one or more previous mobile devices, such as the cellular phones found at his residence.

32. Based on the above, it appears that CAMOVIC was researching law-enforcement-related activity shortly before he attacked the NYPD officers. Furthermore, based on my training and experience, I know that individuals associated with or supporting foreign terrorist organizations and involved in terrorist attacks will sometimes use technology like the Tor network to obtain information and communicate with one another.

33. Also on the CAMOVIC LG Phone was the application Discord, an internet-based communications platform. Discord is an application and digital distribution platform designed for creating communities ranging from gamers to education and businesses. Discord specializes in text, image, video and audio communication between users in a chat channel and allows users to send direct messages to each other. Discord has both a desktop application and a mobile application, and the service can also be accessed from a website.

34. On or about June 8, 2020, law enforcement individuals interviewed an associate of CAMOVIC ("Individual 4").[3] Individual 4 informed law enforcement that he/she and CAMOVIC have been friends since childhood. Individual 4 informed law enforcement that recently, in addition to spending time and playing video games with CAMOVIC, the two also communicated over Discord. Both CAMOVIC and Individual 4 are Muslims, and Individual 4 informed law enforcement that beginning approximately six months ago, he noticed that CAMOVIC was becoming more religiously observant. Individual 4 believed CAMOVIC's becoming more religious was a positive development because, previously, CAMOVIC had a violent temper and often started physical altercations over perceived slights and, as he became more religious, CAMOVIC became less prone to angry outbursts. However, Individual 4 also informed law enforcement that, around the time of Ramadan in approximately April 2020, CAMOVIC used his Discord account to send Individual 4 two videos of a sermon by an imam. Individual 4 informed law enforcement that he/she did not open the videos CAMOVIC sent via Discord because he/she feared that the content of the videos might get Individual 4 in trouble. Individual 4 further

---

[3] The prior search warrant affidavits in this case refer to other associates of CAMOVIC as "Individuals 1, 2, and 3."

informed law enforcement that after CAMOVIC sent him/her the two videos on Discord in or around April 2020, CAMOVIC repeatedly asked Individual 4 if he/she had watched the videos.

35. Records obtained from Discord show that CAMOVIC's account was created on or about February 12, 2017, is registered to CAMOVIC and is associated with CAMOVIC's email address, dzenancamovic123@gmail.com. Records from Discord further show that CAMOVIC used his account numerous times in the days and weeks leading up to his June 3, 2020 attack on NYPD officers. Indeed, the records show that CAMOVIC used Discord at approximately 10:00 p.m. and 11:06 p.m. on June 3, 2020, less than an hour before he attacked the police.

36. The Discord records also contained Internet Protocol ("IP") information for CAMOVIC's account, reflecting that CAMOVIC likely accessed Discord while at the Target Premises. Specifically, CAMVOIC's Discord account repeatedly utilized IP address 67.245.164.101 ("the IP address"), which resolves to Spectrum Communications, Inc., which provides cable and internet service to Jeffersonville, New York, where the Target Premises is located. I have received records from Spectrum Communications, Inc. and the IP address resolves to the Target Premises. Discord records reveal that CAMOVIC's Discord account used the IP address throughout 2020 and as recently as June 1, 2020. Specifically, CAMOVIC's Discord account used the IP address during the following time periods:

- February 16, 2020 through February 17, 2020;
- February 29, 2020 through March 2, 2020;
- March 24, 2020 through May 4, 2020;
- May 9, 2020 through May 11, 2020;
- May 18, 2020;
- May 22, 2020 through May 26, 2020;
- May 30, 2020 through June 1, 2020

As such, CAMOVIC was present at the Target Premises during these time periods.

37. The Discord records show that CAMOVIC's use of Discord immediately prior to the June 3, 2020 attack resolved to an IP address belonging to AT&T, which is the service provider of the CAMOVIC LG Phone.

ELECTRONIC DEVICES AT THE TARGET PREMISES

38. The Target Premises is a three-story residence with a light-colored wood façade, dark shutters and an enclosed front porch.

39. Law enforcement interviewed CAMOVIC's father, Husejin Camovic, after the aforementioned attack. Husejin Camovic stated in substance that he had purchased the Target Premises in October of 2019, and that the Target Premises was used as a second home for their family, where CAMOVIC and others would reside. He further stated that CAMOVIC had recently been staying at the Target Premises since the outset of COVID-19 pandemic and had recently returned to Brooklyn on or about June 1, 2020. This is consistent with the IP address information from CANVOIC's Discord account, as described above. I have reviewed publically-available records for the Target Premises, which show that it is owned by "HUSEJIN CAMOVIC" since at least on or about September 28, 2019.

40. Husejin Camovic further stated in substance that there is an Apple Macbook Pro laptop computer, an Apple desktop computer, and an Apple iPad at the Target Premises, but he was unsure if CAMOVIC had used them.

41. As described above, records regarding CAMOVIC's Discord account show that CAMOVIC was likely at the Target Premises and using an internet capable device—such as a cellphone, laptop or desktop computer—as recently as June, 1, 2020.

42. Based on my training and experience, I know that individuals who provide support to foreign terrorist organizations such as ISIS, as well as individuals who plan and

conduct terrorist attacks, often use multiple cellular phones and other electronic devices. They do so as a form of operational security, to compartmentalize evidence of their criminal activity and prevent the full details of their conduct from being revealed if one device is discovered by law enforcement.

43. Additionally, based on my training and experience, I know that all of the Devices – including cell phones, tablets, external thumb drives, CDs and DVDs – are compatible with or peripherals for an Apple Macbook Pro laptop computer or an Apple desktop computer. Additionally, as stated previously, while a sleeve for a laptop computer was also found in CAMOVIC's bedroom, no laptop was located inside of the Brooklyn apartment. Furthermore, I know that a cell phone, such as the CAMOVIC LG Phone, can be backed up by connecting it to a desktop or laptop computer, such as a MacBook Pro or Apple desktop.

44. As such, I believe the electronic devices are likely to be found in the Target Premises and that they are likely to contain evidence of the Subject Offenses. As described previously, the Devices, CDs and DVDs recovered from CAMOVIC's bedroom contained violent jihadist material. These items necessarily require either a laptop or desktop computer in order to access information on the Devices. Notably, the aforementioned thumb drive contains much of the same material as found on the CDs and DVDs, indicating they were transferred. As stated previously, Discord can be used with any laptop, desktop computer or tablet, such as an iPad.

45. In addition to authorizing the search of the Target Premises for the items described in Attachment B, the requested warrant also authorizes the seizure and search of these and other electronic devices contained therein. Because other people besides CAMOVIC have stayed at the Target Premises, it is possible that the Target Premises will contain storage media

that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

46. As described above and in Attachment B, this application seeks permission to search for evidence that might be found in the Target Premises, in whatever form they are found. One form in which the records might be found is data stored on storage media, such as a tablet, laptop, computer hard drive, or cellular telephone. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. *Probable cause.* I submit that if a computer or storage medium is found in the Target Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

48. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only files that might serve as direct evidence of the Subject Offenses, but also for forensic electronic evidence that establishes how devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Target Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs

may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating

criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

49. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

50. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION AND SEALING

51. Based on the foregoing, I submit that this affidavit establishes probable cause to search the Target Premises, as described in Attachment A, for the items and evidence listed in Attachment B.

52. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. While CAMOVIC is now aware of the investigation, others, known and unknown, with whom he was potentially in contact about the Subject Offenses may not be aware that the government's investigation will continue beyond the arrest of CAMOVIC. Accordingly, there is good cause to seal these documents because their premature disclosure may

seriously jeopardize that investigation. Additionally, the investigation involves the participation of Individual 4 described herein, and release of the information contained in this affidavit could subject Individual 4 to reprisals and harassment, including intimidation designed to prevent Individual 4's further participation in the government's investigation of CAMOVIC and others.

Respectfully submitted,

COLIN J. MCLAFFERTY
Special Agent, FBI

Subscribed and sworn to me by phone
on June 9, 2020:

THE HONORABLE SANKET J. BULSARA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The property to be searched is: the premises known and described as 4956 State Route 52, Jeffersonville, New York 12748, and any closed and locked containers found therein (the "Target Premises"). The Target Premises is a three-story residence with a light-colored wood façade, dark shutters and an enclosed front porch, depicted below:

ATTACHMENT B

Items to be seized from the Target Premises, all of which constitute evidence or instrumentalities of violations federal criminal law by DZENAN CAMOVIC ("CAMOVIC"), among others, including 18 U.S.C. § 231(a)(3) (obstruction of law enforcement officer related to civil disorder), 18 U.S.C. § 922(g)(5) (possession of a firearm by an illegal alien), 18 U.S.C. § 2339B (provision of material support to a foreign terrorist organization), 18 U.S.C. § 1951 (Hobbs Act robbery), and 18 U.S.C. § 924(c) (discharge of a firearm during a crime of violence), (collectively, the "Subject Offenses"), between January 1, 2019 and June 3, 2020.

1. Computers or storage media, including an Apple MacBook Pro laptop, Apple desktop and Apple iPad. For any computer or storage medium whose seizure is authorized by this warrant, and any computer or storage medium (such as tablets, laptops, or cellular telephones) that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "Computer"):

    a. evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. Evidence indicating efforts to provide support to or promote the activities of terrorists and foreign terrorist organizations, including by committing acts of violence in support of such organizations, including the Islamic State of Iraq and al-Sham ("ISIS") and al-Qaeda in the Arabian Peninsula ("AQAP");
    c. Evidence, including messages, videos, communications, audio recordings, pictures, video recordings, or still captured images relating to jihadist propaganda, including communications regarding support for extremist attacks and support for violent extremist groups, including AQAP and ISIS; Evidence regarding CAMOVIC's state of mind, including whether and why he harbored any hostile views toward law enforcement and the NYPD. Evidence of CAMOVIC's close associates, including the individuals with whom he may have had contact in the days leading up to June 3, 2020.evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    d. evidence of the lack of such malicious software;
    e. evidence indicating how and when the Computer was accessed or used to determine the chronological context of Computer access, use, and events relating to crime under investigation and to the Computer user;
    f. evidence indicating the Computer user's state of mind as it relates to the crime under investigation;
    g. evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer;
i. evidence of the times the Computer was used;
j. passwords, encryption keys, and other access devices that may be necessary to access the Computer;
k. documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer;
l. records of or information about Internet Protocol addresses used by the Computer;
m. records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
n. contextual information necessary to understand the evidence described in this attachment.
o. routers, modems, and network equipment used to connect the Computer to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.